Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB04/005179

International filing date: 08 December 2004 (08.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: GB
Number: 0328395.9
Filing date: 08 December 2003 (08.12.2003)

Date of receipt at the International Bureau: 24 January 2005 (24.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/GB 2004 / 0 0 5 1 7 9

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 13 January 2005

THE PATENT OFFICE
D
-8 DEC 2003
LONDON

Patents Form 1/77
Patents Act 1977
(Rule 16)

The Patent Office

090EC03 E857928-54 D02917
P01/7700 0.00-0328395.9

Request for grant of a patent

8 DEC 2003

The Patent Office
Cardiff Road
Newport
South Wales NP10 8QQ

1. Your reference
5489401/JAC/SMT

2. Patent Application Number
0328395.9

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Innovision Research & Technology PLC
Ash Court
23 Rose Street
Wokingham
Berkshire
RG40 1XS

08144784001

Patents ADP number *(if known)*

If the applicant is a corporate body, give the country/state of its incorporation

Country: Great Britain
State: Wokingham, Berkshire

4. Title of the invention
RFID TAGS

5. Name of agent
"Address for Service" in the United Kingdom to which all correspondence should be sent

Beresford & Co
16 High Holborn
London WC1V 6BX

Patents ADP number

6. Priority: Complete this section if you are declaring priority from one or more earlier patent applications filed in the last 12 months.

Country	Priority application number	Date of filing

Patents Form 1/77

7. Divisionals, etc: Complete this section only if this application is a divisional application or resulted from an entitlement dispute.

Number of earlier application	Date of filing

8. Is a Patents Form 7/77 (Statement of inventorship and of right to grant of a patent) required in support of this request?

YES

9. Enter the number of sheets for any of the following items you are filing with this form.

Continuation sheets of this form	0
Description	5
Claim(s)	-
Abstract	-
Drawing(s)	-

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent *(Patents form 7/77)*	1 + 1
Request for preliminary examination and search *(Patents Form 9/77)*	-
Request for Substantive Examination *(Patents Form 10/77)*	-
Any other documents *(please specify)*	NONE

11. I/We request the grant of a patent on the basis of this application

Signature Beresford & Co Date 8 December 2003

BERESFORD & Co

12. Name and daytime telephone number of person to contact in the United Kingdom - JANE CLARK

Tel: 020 7831 2290

5489401

RFID Tags

This document summarises an innovative application technique for protecting functionality of generic Radio Frequency Identification or Identifiable (RFID) tags.

Background:

RFID tags are broadly split into two operational categories; either active or passive. Active tags incorporate an internal battery while passive tags do not require their own energy supply for operation. Passive tags actually operate by extracting their operating power from the RF field emitted by the reader when it is nearby.

The lowest cost category and hence most popular is the passive variety because they are normally smaller and lighter than active tags and do not have any associated lifetime issues due to there being no battery charge to run out.

Any RFID system will contain the following components:-

- Tag (or transponder)
- Reader (or writer/reader)

The transponder or tag will normally consist of an electronic circuit and a coupling device to allow power retrieval from the electromagnetic RF field and communication back to the reader. The tag has a memory where data is stored in a non-volatile form usually under timing and control of a local state machine or logic engine.

The reader sub-system is designed for the requirements of the application and often comprises of the Antenna coil, RF front-end, RF to baseband conversion and a micro-processor for the timing control, intelligence, data decoding and interfacing to the user or other parts of the application system.

As well as supplying power to the transponder, the reader uses the electromagnetic field to exchange data and timing pulses with the transponder. This data exchange would normally involve the reader sending a command to the transponder to ask for the data stored in memory to be sent back, ie "read".

Problem and solution:

The tag functions as a memory store for data and it may have a logically complex configuration of memory types and data usages.

When RFID readers or terminals are available to the mass market in large quantities at the right level of cost then the number and variety of RFID applications will proliferate. In a lot of cases different applications are likely to share common tag components or platforms as well as common reader components and designs. With the use of standards and common/compatible component types comes the risk of unintentional inter-operation. During normal every day use the readers may easily encounter tags which are normally only intended for operation with readers from other different applications. This could be both accidental and user intentioned for a variety of different motives.

One of the problems resulting is that application B will interpret the stored data differently to application A. If the application B is capable of changing data in a tag originally used on application A, ie a Write function, then application B will write differently to application A and would therefore corrupt the data. When this tag is re-used back on an application A reader then the data would most likely be lost or corrupted resulting in unexpected operation and serious loss of information.

Typically the tags; be they Read Only or User Read/Write or a combined mixture, are released to the users of an application in a number of ways;

(i) Always intended for operation with that specific application only, with some or all data already installed, either formatted, pre-configured and initialized.
(ii) Generic tag ready for use and re-use across a number of applications, normally formatted but blank.
(iii) Generic tag ready for use across a number of applications but once used must be fixed or allocated solely to that application.

Therefore, it is clear that there needs to be a way to ensure these options; for example that a generic tag once used for one application can only in future be re-used on that same application to avoid functionality problems as discussed above. The suggested solution is the use of a PIN number or application specific code number or series of multiple numbers to enable tag operation only for the intended application. In fact the method may be extended to use different numbers for enabling different levels of operation eg Read Only or Read & Write functionality and may even be restricted to only specific areas or all of the tag memory. The hidden numbers may also be used to customise tag configuration and enable customisation of permitted operational features.

On an individual level there are also applications where a user wishes to for example store personal data onto a tag in the knowledge that other users, should they gain possession of the tag, cannot ever access the data. Only the true owner or a 3rd party only with their express permission can access the tag.

The suggested solution is the ability to choose and then install a PIN number or "Pass Code" into the tag. Then, in order to subsequently access the data in the tag, the correct PIN number must first be entered by the user into the reader, (or else called up from local storage), to be used to enable access permission to the tag for reading and/or writing transactions.

Again the method may be extended to use different PIN numbers for enabling different levels of Read Only or Read & Write functionality maybe for different specified areas of tag memory.

Background assumptions:

Currently RFID tags have various types of memory functionality, which include;

Read Only
This is normally implemented either by means of custom metal mask layers fixed at design time for Read Only Memory, (ROM), or by EEPROM Read/Write memory which is written too and then locked from further write operations either during

manufacture or at an initialisation stage prior to delivery or at some other time in the life-cycle of the tag.

Read/Write many times (R/W)
This is normally implemented by use of Electrically Erasable Memory, (EEPROM), whereby during a write sequence the contents of the memory byte or bytes are first erased and then written to for the purposes of storing new information.

Write Once Read Many (WORM) or One Time Programmable (OTP)
This can be realized within a tag either using the EEPROM memory but with the erase disabled so that once written to, ie bits have changed state they can no longer be changed back again. These can be considered at the byte level or the individual bit level. Alternatively, an OTP functionality can be achieved by some form of fuseable link where electrical current is used to melt and physically destroy a metal or poly-metal link to open circuit a connection and irreversibly change the logic state of each individual bit.

Details of Application Invention:

This application invention covers the usage of another type of memory to implement a PIN number and Pass Code function as follows.

Write Only Memory (WOM)
Under certain circumstances this type of tag memory can be written to and is non-volatile but cannot normally ever be read back externally from the tag. Therefore once written to, it's contents are protected and remain secret from external parties.

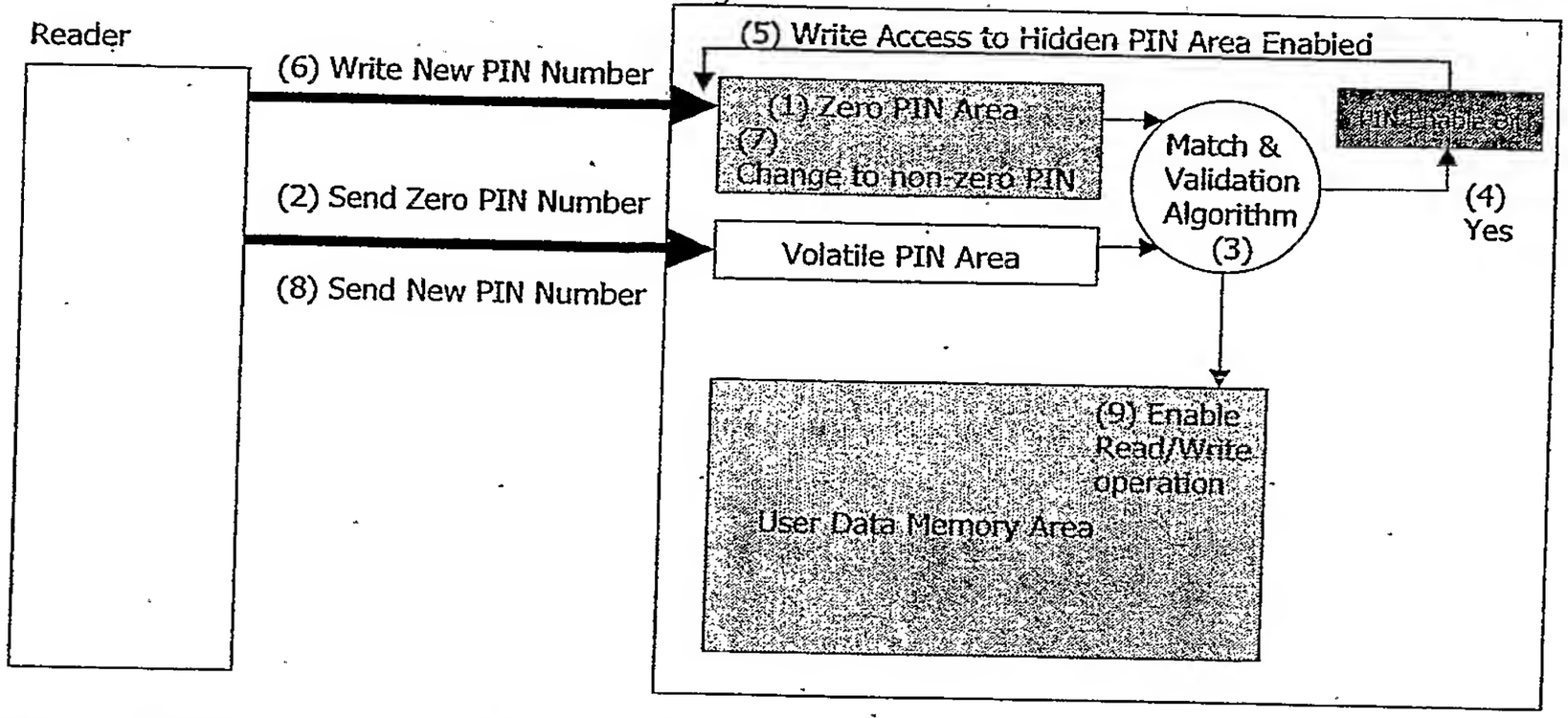
However, the internal circuitry and state machine of the tag can still read the contents locally and then use this information within an algorithm to perform the authentication and access control rights to enable the permitted functionality during transactions. This algorithm could include data from a combination of all or some of; multiple hidden areas, the Unique Identification (UID) number of the tag, actual tag data and digital signature data.

The WOM memory function can be implemented using normal EEPROM which has associated address decoding and control logic to permanently stop operation of external read functions. It can also have logic to selectively enable the Write function only under certain qualifying pre-conditions.

Explanation of PIN Number protection Method using WOM:

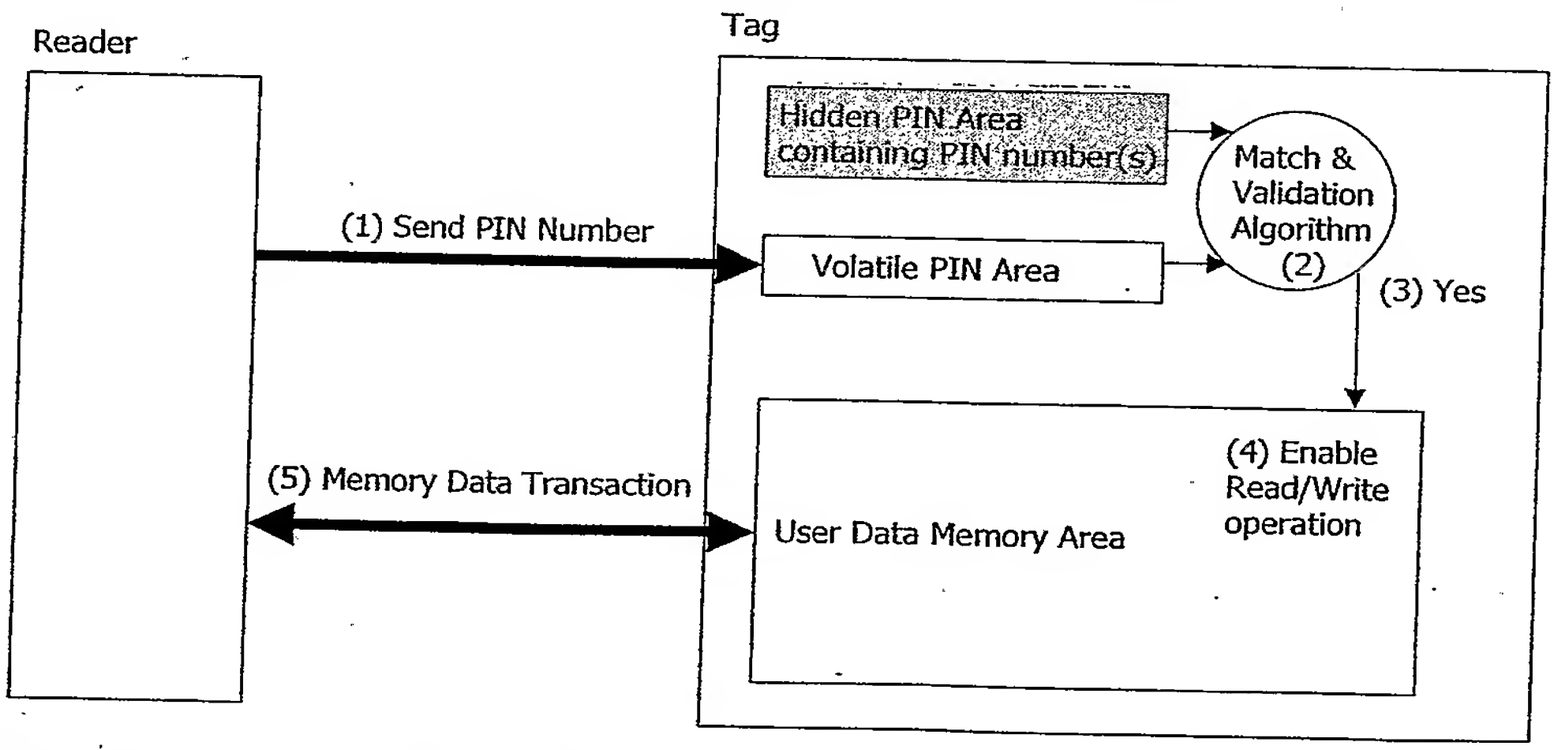
When first manufactured and in some applications delivered to the user the PIN number function could be disabled and the tag operates normally and memory access is fully available and transparent to the user. At some stage in the life-cycle of the tag either during manufacture, initialization or user required then a single or multiple PIN numbers can be installed as follows, see Figure 1.

Figure 1 – Sequence of Installing the 1st PIN Number



(1) The Hidden PIN area is initially set at a default value, say zero.
(2) Send zero pin number.
(3) Match and validation algorithm runs internally on tag.
(4) Correct match and updating of stored PIN is enabled.
(5) Write access is allowed to change the PIN.
(6) User installs their PIN number or numbers.
(7) New PIN number(s) are written into hidden memory.

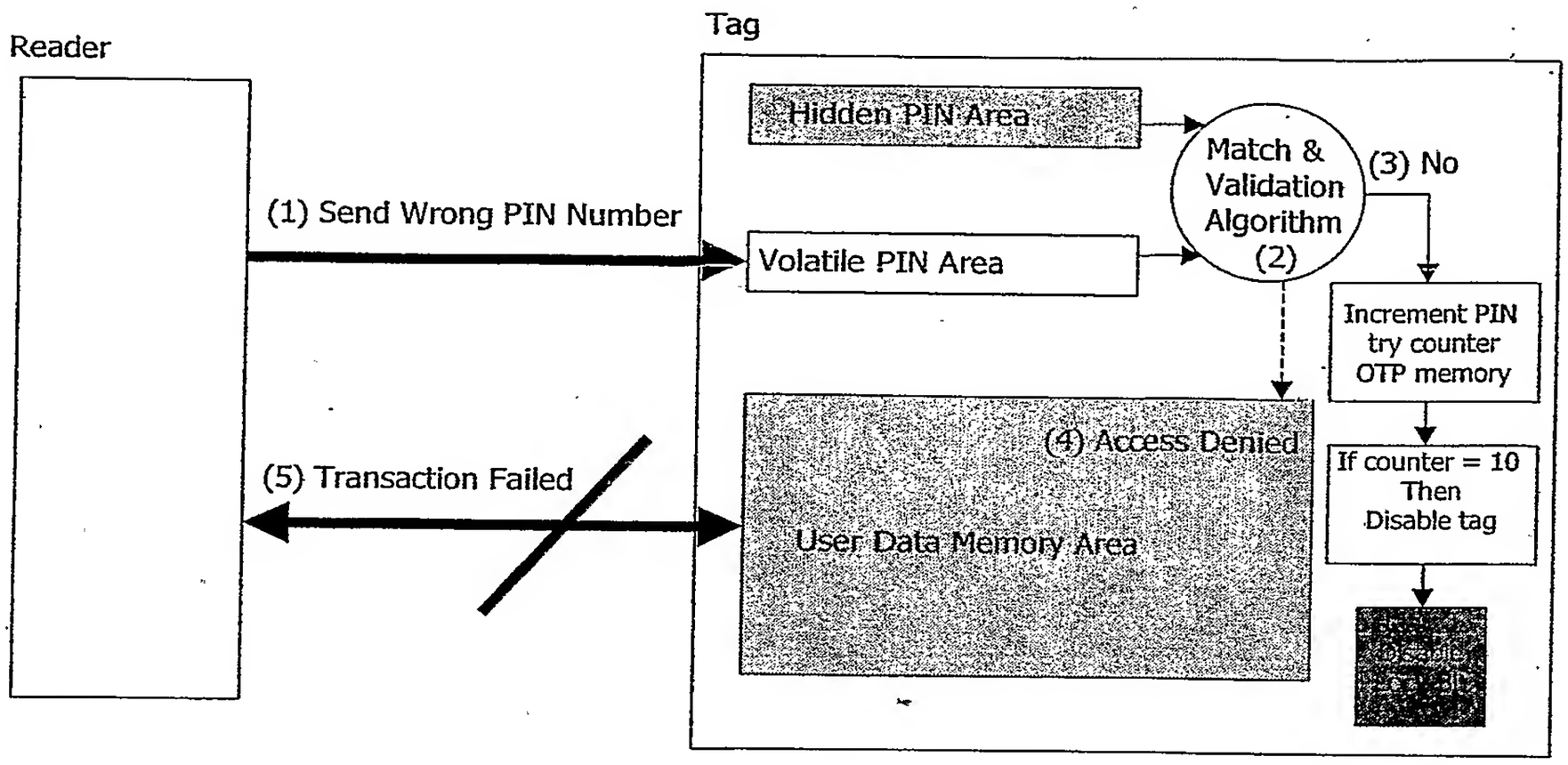
Figure 2 – Sequence of Subsequent PIN Number Operation



(1) User sends candidate PIN number to temporary volatile store area.
(2) Match and validation algorithm runs internally on tag.
(3) Correct match, (If not correct see figure 3 below).
(4) Enables Read/Write operation to take place for this transaction.
(5) Tag memory data transaction performed.

After completion of the transaction and when tag is powered down the contents of the volatile PIN area and the enable function will naturally disappear.

Figure 3 – Sequence of Operation Using Invalid PIN Number(s)



(1) User sends candidate PIN number to temporary volatile store area.
(2) Match and validation algorithm runs internally on tag.
(3) NOT a correct match, the *try counter* is incremented in an "OTP fashion".
(4) Access denied.
(5) Tag transaction fails.
(6) As long as *try counter*<10 then PIN number entry can be tried again.

The *try counter* is used to prevent hackers from just cycling through all of the possible combinations of PIN numbers or multiple PIN numbers. After say, the 10^{th} try at guessing the correct PIN number, the tag is locked in the disabled state and the tag is now useless and data is permanently inaccessible.

Prior to reaching the 10^{th} try if in fact the correct PIN number is successfully entered at any stage then the *try counter* "OTP" memory can be reset back to zero count again.

Additionally, certain applications may have a function enabled whereby it is possible to erase the whole tag memory completely, (except UID), in this case all sensitive data is deleted, the PIN number resets to default and the tag reverts back to it's initial blank state so that the tag can be ready for use over again. This would at least make the tag re-useable in the case where the user forgets the PIN number.

Ian K.